Hastings Communications and Entertainment Law Journal

Volume 10 | Number 3 Article 1

1-1-1988

In the Ordinary Course of Business: The Legal Limits of Workplace Wiretapping

Martha W. Barnett

Scott D. Makar

"In the Ordinary Course of Business": The Legal Limits of Workplace Wiretapping

by MARTHA W. BARNETT*
and
SCOTT D. MAKAR**

Table of Contents

* Partner, Holland & Knight, Tallahassee, Florida. Board of Governors, American Bar Association. B.A., H. Sophie Newcome Memorial College, 1969; J.D., University of Florida, 1973.

** Visiting Assistant Professor, Business Law, College of Business Administration, University of Florida. B.S., Mercer University, 1980; M.B.A., 1982, M.A., 1982, J.D., 1987, University of Florida. The authors express appreciation to the Public Utility Research Center, University of Florida, for its support.

Introduction

The expanded use of telecommunications monitoring and recording devices in the workplace has incited an impassioned controversy.[1] At odds are employees' privacy interest[2] in their

1. The controversy is part of a perceived decline in ethical behavior both in and out of the workplace. *See, e.g., Executives and General Public Say Ethical Behavior Is Declining in U.S.*, Wall St. J., Oct. 31, 1983, at 33, col. 3. A Gallup Poll commissioned by the Wall Street Journal indicated 65% of those individuals surveyed (general public citizens and business executives) think the overall level of ethics in American society has declined in the past decade while only 9% say it has risen. *Id.* The poll found that 49% of the general public, as compared with only 23% of business executives, believed ethic standards in business had declined. Furthermore, 78% of the executives, compared with 15% of the general public, stated they had used a company telephone for unauthorized personal long-distance calls. *Id.* This divergence between belief and behavior indicates a possible "double-standard" in the workplace. There are also potential adverse physical side-effects to workplace monitoring. *Employer Eavesdropping*, 73 A.B.A. J. 24-25 (1987) ("Employees in monitored jobs suffer increased levels of stress-related illnesses like ulcers, heart disease, anxiety, fatigue, high blood pressure, diabetes and depression.").

2. The term "privacy" is vague and highly emotive. Many commentators have made efforts at defining privacy and its various components. *See, e.g.*, S. BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 10-11 (1982) (privacy is "the condition of being protected from unwanted access by others — either physical access, personal information, or attention"); R. POSNER, THE ECONOMICS OF JUSTICE 231 (1981) (author discusses three meanings of privacy: secrecy, seclusion, and autonomy). An employee's particular privacy interest in workplace communications on a company phone is primarily a "secrecy" interest defined as the withholding or concealment of information or personal facts from others. *Id.* at 231.

Companies or individuals may attempt to obtain information about a person's affairs so they can gain a personal, social, or economic advantage. For example, "[p]rying enables one to form a more accurate picture of a friend or colleague, and the knowledge gained is useful in social or professional dealings with him." *Id.* at 232. One state has enacted a provision prohibiting employer "prying." *See* MICH. COMP. LAWS ANN. § 423.508 (West 1987) (prohibiting employer from creating a record of employee's "non-employment activities" unless authorized by the employee or occurring in the workplace). Withholding or concealing personal information allows a person to control other people's opinions about that person. This secrecy interest, however, does not appear to be absolute. For example, when the information an employee attempts to keep secret from his employer directly affects a legitimate business interest, the business's interest may override the employee's secrecy interest. *See, e.g.*, Briggs v. American Air Filter Co., 630 F.2d 414 (5th Cir. 1980) (employer monitoring phone conversation of employee leaking confidential information). Conversational privacy also increases the informational content of personal communications by increasing a speaker's brevity and informality. R. POSNER, *supra*, at 247. The lack of such privacy imposes costs in the form of (1) greater deliberation time in deciding what to say to prevent disclosing personal information or offending someone else; and (2) reduction in precision and lucidity of thought. *Id.* at 245.

workplace communications and businesses' interest in reducing the costs associated with employee misuse of their telecommunications system.[3] These conflicting values are evidenced in the dramatic increase in employee suits alleging invasion of privacy by employers.[4] In addition, employee organizations are lobbying legislators to pass laws eliminating all or most forms of wire and electronic surveillance.[5] Employers counter that employee monitoring methods are necessary to maintain their companies' competitive viability.[6] They point out that employee supervision has always been a business's responsibility whether to improve worker performance or to prevent malingering or theft.[7] The advent of modern scientific management theory,[8] along with newly developed monitoring technologies,[9]

3. One poll addressed the ethical issue of how large the costs of unauthorized telephone use must be before business executives become concerned. Ricklefs, *Executives Apply Stiffer Standards Than Public to Ethical Dilemmas*, Wall St. J., Nov. 3, 1983, at 33, col. 4. The Gallup Poll asked whether an employee who discovers that a fellow employee has been sneaking $100 of unauthorized calls per month should report the employee to the company. Seventy-six percent of business executives indicated the employee should be reported while 19% favored disregarding the matter. The figures for the general public were 64% and 26% respectively. When the amount of calls was $10 per month, however, the figures fell to 48% and 47% respectively for business executives and 47% and 38% respectively for the general public. *Id.*

4. *See generally*, WORKPLACE PRIVACY: EMPLOYEE TESTING, SURVEILLANCE, AND WRONGFUL DISCHARGE AND OTHER AREAS OF VULNERABILITY (BNA) 107-46 (1987) (special report compiling cases involving workplace privacy issues).

5. *See, e.g., "Don't Bug Me" (Communications Workers of America Fights for Passage of a Bill Prohibiting Secret Electronic Monitoring of Workers Using Computers or Telephones)*, Wall St. J., Apr. 21, 1987, at 1, col. 5. Currently, Congress is considering passage of a "beep bill" which would require that telephone monitoring by employers be accompanied by an audible warning tone. *See infra* note 132 and accompanying text.

6. The business justifications for monitoring activities focus on increasing the economic efficiency of providing goods and services to the public. Call monitoring allows a business to increase or maintain customer satisfaction through the use of employee performance checks. Second, it enables businesses to identify and develop areas in which customers seek further assistance, such as additional telephone services and new product development. Knowing what its customers demand is critical to a business's survival.

7. *See, e.g.*, Brophy, *Putting Social Calls on Hold; Bosses Have a New Weapon in Fighting Phone Bills*, U.S. NEWS & WORLD REP., Sept. 29, 1986, at 54-55. Apparently, employee misuse of the company's telephone system is very common. One estimate of the percentage of calls not related to work ranges from 10% to 30% at private companies. *Id.* at 54. In addition, a government survey found that 29% to 50% of long distance calls by employees were personal rather than business. *Id.*

8. Scientific management theories, which focus on increasing worker productivity through techniques such as time and motion studies, have become popular methods of facilitating managerial control.

9. *See, e.g.*, Budiansky, *Cheaper Electronics Makes It a Snap to Snoop*, U.S. NEWS & WORLD REP., May 18 1987, at 54 (new technology makes it possible to tap phone

makes it inevitable that the already pervasive monitoring and recording of telephone communications in the workplace will increase.[10]

Private businesses that want to monitor or record workplace telephone messages are subject to numerous perils under both federal and state law. Federal wiretapping laws[11] and Federal Communications Commission (FCC) rules[12] regulate the circumstances and methods by which recording or monitoring may occur. The federal wiretapping laws, though primarily directed at government law enforcement activities, also apply to surveillance activities conducted by businesses or individuals. These laws, however, have statutory exceptions which permit the monitoring or recording of communications "within the ordinary course of business"[13] or when one or more parties consent.[14] Federal courts have inconsistently interpreted these exceptions, with some courts emphasizing the lessened privacy expectations of the telephone users,[15] and other courts emphasizing that the workplace communications "were in the ordinary course of business."[16] This uncertainty blurs the permissible limits of business monitoring in various jurisdictions.

A person's general right to privacy is left largely to the law of

---

lines without physical penetration into wire). *High-Tech Big Brother,* SCI. AM., Jan. 1986, at 60 (citing examples of the "virtual revolution in the technology relevant to electronic surveillance").

10. An estimated 15 million workers are potentially subject to electronic workplace monitoring, according to the Communications Workers of America. *See Employer Eavesdropping,* 73 A.B.A. J. 24 (1987). Many of these employees are telephone sales representatives or employees of telecommunications service providers. Another indication of this expansive trend is the increased sales of station message detail recording (SMDR) devices, which allow the programmed monitoring and recording of calls on business systems. In 1985, over 20,000 SMDR and related systems were sold in the United States. *See* Marx & Sherizen, *Corporations That Spy on Their Employees,* 60 BUS. & SOC'Y REV., Winter 1987, at 32. Because the cost of surveillance technology is declining rapidly, more businesses will purchase and use such devices. Budiansky, *supra* note 9, at 54-56.

11. *See infra* notes 28-54 and accompanying text.

12. The FCC has adamantly upheld its position as protector of individual privacy interests in interstate communications despite a preemption issue lurking in the background of its most recent rule regarding permissible recording methods. *See infra* notes 145-54 and accompanying text.

13. *See infra* notes 55-72 and accompanying text.

14. *See infra* notes 114-20 and accompanying text.

15. *See infra* notes 137-43 and accompanying text.

16. *See infra* notes 73-113 and accompanying text (discussing the "context" and "content" approaches courts use to analyze the ordinary course of business exception).

the individual states.[17] Some states have constitutional provisions, statutes, or common law that protect individual privacy interests.[18] Generally, these laws are more expansive and protective of a person's privacy expectations than federal laws. Florida, for example, has a stringent requirement that all parties to a communication must consent before monitoring or recording can be accomplished.[19] In addition, state public service commissions impose tariff provisions on telephone companies, requiring them to discontinue service to businesses that engage in prohibited methods of surveillance.[20] The net result is an interlocking and overlapping web of federal and state laws which limits the extent to which businesses may monitor and record intrastate and interstate telephone communications on their phone systems.

This article analyzes the federal and state laws[21] that limit the extent to which a private employer may monitor [22] or record[23] phone messages transmitted or received on the em-

17. Katz v. United States, 389 U.S. 347, 350-51 (1967).

18. *See generally* Note, *Toward A Right of Privacy As A Matter of State Constitutional Law*, 5 FLA. ST. U.L. REV. 631 (1977) (overview of states having "free-standing" right of privacy and right of privacy explicitly or implicitly in unreasonable search and seizure provisions). *See also infra* notes 158-61 and accompanying text (discussing state constitutional provisions); notes 161-208 and accompanying text (discussing state statutory provisions).

19. FLA. STAT. ANN. § 934.03(2)(d) (West 1985). *See* discussion *infra* notes 193-202 and accompanying text.

20. *See infra* notes 211-14 and accompanying text.

21. This article discusses federal statutory law and administrative regulations. *See infra* notes 29-151 and accompanying text. In addition, Florida constitutional, statutory and administrative provisions are included as examples of state law.

State tort law protections based on invasion of privacy claims are not discussed in detail. Prior to the enactment of state statutory provisions, state tort law had traditionally been used to protect the wrongful interception of private workplace communications. The principle that the wrongful intrusion into physical solitude or seclusion violates the right of privacy has been extended by many courts to include eavesdropping on private conversations. *See* W. KEETON, D. DOBBS, R. KEETON & D. OWEN, PROSSER & KEETON ON THE LAW OF TORTS 854-55 (5th ed. 1984). For an overview of the tort law applicable to wiretapping, see generally Annotation, 11 A.L.R. 3D 1296 (1967 & Supp. 1987) (annotation of eavesdropping as a violation of the right of privacy).

22. "Monitoring" refers to listening in on others' wire communications contemporaneously by means of a wiretap device. The situation where an individual listens to a recordation of a wire communication at a later time is included within the definition of "recording." *See infra* note 23.

23. "Recording" means the act of using a device to acquire and reproduce the sounds contained in a wire communication. Under the various statutes, unauthorized recording is actionable even though there is no use or disclosure of the contents of the recorded conversation. *See infra* notes 34, 145-54 and accompanying text.

ployer's telecommunications system.[24] In particular, situations where employers use monitoring or recording as a service quality assurance measure or to prevent unauthorized use are considered. The article examines tensions between FCC rules and the federal and state wiretapping statutes with particular emphasis on the "ordinary course of business" and "participant consent" exceptions. The article then analyzes cases in which courts attempt to interpret statutes that sometimes seem incongruous.[25] A brief analysis of a proposed federal "beeper" bill is also presented.[26] The article includes some recommendations on how businesses can avoid the legal pitfalls awaiting the unwary.[27]

I
Federal Law

A. Omnibus and Privacy Acts

The primary federal wiretapping statute is the Omnibus Crime Control and Safe Streets Act of 1968[28] (Omnibus Act), which was amended by the Electronic Communications Privacy

24. This article's analysis is limited to private employers. In cases involving public employers, the fourth amendment guarantee against unreasonable searches and seizures would also apply. *See* O'Connor v. Ortega, 107 S. Ct. 1492 (1987). Balancing the government's need for supervision, control, and efficiency in the workplace against employees' privacy rights, a plurality of the U.S. Supreme Court held that a standard of reasonableness for evaluating searches of public employees' offices by their employers would not unduly burden government employers' interests nor authorize arbitrary intrusions upon public employees' privacy rights. *Id.* at 1502.

25. Judge Arthur Goldberg, attempting to interpret the federal wiretapping statute, said the following:

> We might wish we had planted a powerful electronic bug in a Congressional ante chamber to garner every clue concerning Title III [the federal wiretapping statute], for we are once again faced with the troublesome task of an interstitial interpretation of an amorphous Congressional enactment. Even a clear bright beam of statutory language can be obscured by the mirror of Congressional intent. Here, we must divine the will of Congress when all recorded signs point to less than full reflection. But, alas, we lack any sophisticated sensor of Congressional whispers, and are remitted to more primitive tools. With them, we can only hope to measure Congress' general clime. So we engage our windvane and barometer and seek to measure the direction of the Congressional vapors and the pressures fomenting them. Our search for lightning bolts of comprehension traverses a fog of inclusions and exclusions which obscures both the parties' burdens and the ultimate goal.

Briggs v. American Air Filter, Co., 630 F.2d 414, 415 (5th Cir. 1980). The issues in this article should be read with Judge Goldberg's message in mind.

26. *See infra* notes 132-36 and accompanying text.

27. *See infra* notes 229-30 and accompanying text.

28. 18 U.S.C. §§ 2510-25 (1987).

Act of 1986[29] (Privacy Act). The Omnibus Act creates and defines the federal eavesdropping[30] and wiretapping[31] causes of action. Because its original provisions relate to the means of communication prevalent in 1968, the Act originally failed to cover many of the newly developed and sophisticated electronic means of communication.[32] The Privacy Act was passed to rectify this problem by modifying various provisions of the Omnibus Act. In particular, the Privacy Act expanded protection to "electronic" communications as well as wire or oral communications.[33] The Omnibus Act proscribes the illegal interception,[34] disclosure,[35] or use[36] of a wire,[37]

29. Pub. L. No. 99-508 (codified as amended at 18 U.S.C. §§ 2510-3126 (1987)).

30. The term "eavesdropping" is sometimes used to describe "all forms of artificial surveillance of communications." *See* C. FISHMAN, WIRETAPPING AND EAVESDROPPING 4-5 (1978). However, "eavesdropping," as used in this article, refers to any form of nonconsensual surveillance of oral communications other than wiretapping. This definition conforms to what one commentator terms "bugging." *Id. See also* J. CARR, THE LAW OF ELECTRONIC SURVEILLANCE § 1.01[1][a] - [b] (1977) (bugging refers to overhearing, broadcasting, or recording a speaker's conversation). Generally, eavesdropping activity involves the use of an electronic device that enables a listener to hear a conversation without tangible penetration into either a wire or the physical area where the conversation occurs. *See* Note, *Electronic Monitoring in the Workplace: The Need for Standards*, 52 GEO. WASH. L. REV. 438, 439 n.9 (1984).

31. "Wiretapping" generally refers to physical entry into a telephone circuit to intercept a conversation. *See Note, supra* note 30, at 439. Some methods of surveillance do not fit squarely within the definitions of eavesdropping or wiretapping. For example, induction coils allow the interception of wire communications without physical entry into a phone system.

32. Wiley & Leibowitz, *The Electronic Communications Privacy Act of 1986 Moves Privacy Protection Towards the 21st Century*, 4 TELEMATICS 2 (Feb. 1987).

33. For simplification, references hereafter to the Omnibus Act refer to the 1968 Act including the Privacy Act amendments.

34. 18 U.S.C. § 2511(1)(a) (1987). The term intercept is defined in 18 U.S.C. § 2510(4) (1987); *see infra* text accompanying note 56.

35. 18 U.S.C. § 2511(1)(c) (1987).

36. *Id.* § 2511(1)(d). This section, which prohibits the use of the *content of an unlawfully intercepted communication*, should not be confused with section 2511(1)(b), which prohibits the use of particular *devices*.

37. A "wire communication" means:

> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit.

Id. § 2510(1).

oral[38] or electronic[39] communication.[40] A prima facie violation would be: 1) defendant's intentional or willful; 2) interception, disclosure or use; of 3) plaintiff's wire, oral or electronic communication; whose 4) interception occurred on the premises of a business the operation of which affected interstate commerce.[41] Because of the surreptitious nature of the wiretapping tort, courts have generally set forth lenient evidentiary standards that plaintiffs must meet to get a wiretapping case to a

38. An "oral communication" means "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." *Id.* § 2510(2).

39. An "electronic communication" means:

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate commerce, or foreign commerce, but does not include:
>
> (A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;
>
> (B) any wire or oral communication;
>
> (C) any communication made through a tone-only paging device; or
>
> (D) any communication from a tracking device (as defined in section 3117 of this title).

Id. § 2510(12).

40. *Id.* § 2511.

41. United States v. Duncan, 598 F.2d 839, 847 (4th Cir. 1979), *cert. denied*, 444 U.S. 871 (1980). Since Congress intended to prohibit electronic eavesdropping to the full extent of its constitutional authority, the Omnibus Act applies to most, if not all, intrastate phone communications. *Id.* at 854-55. *See* Benanti v. United States, 355 U.S. 96, 104-05 (1957); Weiss v. United States, 308 U.S. 321, 327-29 (1939) (inability of the parties to distinguish between interstate and intrastate communications).

In some situations, a plaintiff may file a claim based on state law alleging the defendant unlawfully monitored an interstate phone call. In this situation, the issue arises regarding which state's wiretapping laws apply. For example, in Becker v. Computer Sciences Corp., 541 F. Supp. 694 (S.D. Tex. 1982), a former employee brought suit for wrongful termination. Through discovery, the defendant-employer discovered that the plaintiff had secretly made tape recordings of conversations between the plaintiff in Texas and the defendant's employees in California. The court found that under Texas law, there is no remedy for the surreptitious recordation of telephone conversations where only one party to the conversation consents. Under California law, however, the court felt that all-party consent is required. The plaintiff urged that enforcement of the California law would violate Texas public policy. The court stated that "[t]he fact that the State of California has sought to protect its citizens' rights to privacy to a greater degree than the State of Texas . . . does not provide a sufficient basis to support a finding that the California statute violates" the public policy of Texas. *Id.* at 703. The court then held that under Texas choice-of-law analysis, which uses a "most significant relationship" test, the California law should apply. *Id.* at 703-06. The court relied upon various sections of the RESTATEMENT (SECOND) OF CONFLICT OF LAWS §§ 6, 145 & 152 (1971) which provides the structure for choice-of-law analysis in such situations.

jury.[42] Courts generally will allow a case to survive motions for a directed verdict or summary judgment even if there is only circumstantial evidence of the defendant's involvement.[43]

The Act's use and disclosure prohibitions apply to business only when a company using or disclosing a communication knew or had reason to know that the communication was intercepted in violation of the Act.[44] The Act itself does not address the use or disclosure of *lawfully* intercepted communications. For example, a business may legitimately monitor communications on its phone system under the "ordinary course of business" exception to the Act. In such a case, there is no "interception" in violation of the Omnibus Act. The business would have a qualified privilege to internally use the content of the communication for a proper business purpose. However, the business may be subject to liability under state tort law theories for improperly using or disclosing the contents of the monitored communication for a non-business purpose.[45] Defamation and invasion of privacy claims could result from public disclosure of particular communications involving employees or other persons.[46] The most common situations would involve employers monitoring the communications of employees[47] or

42. Courts disagree on whether a plaintiff must allege and prove that the defendant illegally intercepted plaintiff's specific communication. Some courts only require a general showing that the defendant engaged in wiretapping activities. Awbrey v. Great Atl. & Pac. Tea Co., 505 F. Supp. 604, 606-07 (N.D. Ga. 1980); *cf.* Oliver v. Pac. Northwest Bell Tel. Co., 632 P.2d 1295, 1299 (Or. 1981).

43. *See* Scutieri v. Paige, 808 F.2d 785 (11th Cir. 1987) (court addressed the issue of the amount and type of evidence a plaintiff must produce to withstand a directed verdict). *See also* Abel v. Bonfanti, 625 F. Supp. 263 (S.D.N.Y. 1985) (grant of summary judgment improper where genuine issue of material fact existed as to whether employer's recording of employee's telephone call was in ordinary course of business); *cf.* MICH. COMP. LAWS ANN. § 750.539i (West Supp. 1987) (proof of installation of intercepting device is prima facie evidence of violation).

44. 18 U.S.C. § 2511(1)(c) - (d) (1987).

45. *See* Ribas v. Clark, 38 Cal. 3d 355, 360-62, 696 P.2d 637, 640-41, 212 Cal. Rptr. 143, 146-47 (1985) (making a distinction between first-hand dissemination of information, which the wiretap laws govern, and second-hand repetitions, which state tort law governs). *Cf.* KY. REV. STAT. ANN. § 526.070 (Michie/Bobbs-Merrill 1984) (inadvertent overhearing of a communication without later divulging its contents is not an eavesdropping violation).

46. The "public disclosure of private facts" breach of privacy tort might apply in certain situations. *See* Beard v. Akzona, Inc., 517 F. Supp. 128, 132 (E.D. Tenn. 1981).

47. *See id.* (employee's action against former employer for invasion of privacy not supported by evidence of willful use in violation of Omnibus Act); Awbrey v. Great Atl. & Pac. Tea Co., 505 F. Supp. 604 (N.D. Ga. 1980) (employees not required to produce evidence of specific instances of eavesdropping; general allegations of employer installing wiretap sufficient to maintain action); Bianco v. American Broadcasting

customers that call the business.[48]

The Act also prohibits the use of any electronic, mechanical, or other device to intercept any oral communication in particular situations.[49] Criminal violators are subject to fine and/or imprisonment up to five years.[50] Additionally, the Act authorizes a civil action[51] to recover compensatory damages,[52] punitive damages,[53] attorney's fees and other litigation costs.[54]

1. *"Extension Phone" and "Ordinary Course of Business" Exceptions*

The prima facie case encompasses an extremely broad range of communications, including a number of legitimate business activities. Under the Act, however, definitions of particular key terms create exceptions in certain situations.[55] Specifically, the Act defines the term "intercept" as the "aural or other ac-

Co., 470 F. Supp. 182 (N.D. Ill. 1979) (employer's electronic eavesdropping did not violate state constitution, which did not apply to private eavesdropping); Simmons v. Southwestern Bell Tel. Co., 452 F. Supp. 392 (D. Okla. 1978) (telephone company employee not entitled to recover for company's monitoring activities because warning about personal calls and notice of monitoring was given).

48. *See, e.g.*, Awbrey v. Great Atl. & Pac. Tea Co., 505 F. Supp. 604 (N.D. Ga. 1980) (individual who called employee at work on line the employer tapped has a cause of action despite not being an employee).

49. 18 U.S.C. § 2511(1)(b) (1987).

50. *Id.* § 2511(4).

51. *Id.* § 2520. Any person whose wire, oral, or electronic communication was unlawfully intercepted, disclosed, or intentionally used may recover damages in a civil action from the person or entity which engaged in the violation. *Id.* Private remedies under the Omnibus Act supersede any private remedies contained in 47 U.S.C. § 605 (1982). Congress did not intend duplicative remedies, since section 605, which prohibits the interception and divulgence of wire and radio communications, was extensively revised by the Omnibus Act. Watkins v. L.M. Berry Co., 704 F.2d 577, 580 (11th Cir. 1983). The civil statute of limitations is two years after the date upon which the claimant first had a reasonable opportunity to discover the violation. 18 U.S.C. § 2520(e) (1987).

52. 18 U.S.C. § 2520 (b)(2) (1987). The measure of damages, exclusive of punitive damages, is the greater of actual damages plus profits made by the violator as a result of the violation or statutory damages (the greater of $100 per day for each day of the violation or $10,000). *Id.* § 2520(c)(2)(A) - (B). This measure of damages is consistent with the tort in some states, which permits the recovery of punitive damages without recovery of actual damages. *See, e.g.*, Scalise v. National Util. Serv., 120 F.2d 938 (5th Cir. 1941) (rule in Florida and federal courts is that an award of punitive damages only requires that plaintiff be subject to a deliberate wrongful act). The theory is that the invasion of a plaintiff's privacy interest is by itself a harmful act requiring compensation despite the lack of actual monetary loss.

53. 18 U.S.C. § 2520(b)(2) (1987).

54. *Id.* § 2520(b)(3).

55. The flow chart in Diagram One in the Appendix illustrates the various paths to Omnibus Act liability or exceptions.

quisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device."[56] Both eavesdropping and wiretapping offenses require that a plaintiff demonstrate the defendant illegally "intercepted" plaintiff's communication by using an "electronic, mechanical or other device." Absent proof that the defendant used a statutorily defined "intercepting device," the plaintiff fails to establish a violation.

An intercepting device may be any "electronic, mechanical, or other device."[57] However, the definition excludes:

> any telephone or telegraph instrument, equipment or facility, or any component thereof, furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business.[58]

This provision, termed the "extension phone" or "ordinary course of business" exception, ostensibly excepts particular devices but actually excepts particular activities.[59] Facially, the statute seems to require that a defendant demonstrate that a purported interception be both in the ordinary course of business and by means of an authorized device.

The typical monitoring method employers use is an extension phone or other similar device. Cases involving the use of extension phones generally conclude that recording a private conversation without the employee's consent[60] is not within the "ordinary course of business."[61] Some courts, however, hold

---

56. 18 U.S.C. § 2510(4) (1987).

57. *Id.* § 2510(5).

58. *Id.* § 2510(5)(a). Notable is that the statute excepts the use of devices provided by either a provider of wire or electronic communication services or the subscriber itself. Thus, under the Omnibus Act, the subscriber can purchase a monitoring or recording device from businesses other than the telephone company. However, the Florida Security of Communications Act, discussed *infra* notes 163-210 and accompanying text, does not include this option. *Cf.* N.H. REV. STAT. ANN. § 570-A:1(IV)(a)(2) (1974), which provides that a phone or other instrument is not an intercepting device if purchased, rented or used by the subscriber or user.

59. These exceptions are theoretically and analytically different from one another, although courts tend to refer to them synonymously.

60. An employer's use of an extension phone may be permissible under the Omnibus Act's participant consent exception, discussed *infra* notes 193-202 and accompanying text.

61. *See, e.g,* United States v. Harpel, 493 F.2d 346, 351 (10th Cir. 1974). *Harpel*

that the Omnibus Act exempts interceptions made with extension phones because they are not "intercepting" devices within the meaning of the statute.[62] This latter perspective conflicts with the principle that the application of the Omnibus Act "should not turn on the type of equipment that is used, but whether the privacy of telephone conversations has been invaded in a manner offensive to the words and intent of the Act."[63] In the business context, the better view accords with this principle: an interception by means of an extension phone (or other permissible device) must also be in "the ordinary course of business" for the statutory exception to apply.[64] An employer cannot engage in nonconsensual surveillance and invade employees' privacy interests by simply using an extension phone.

Employees' expectations of privacy[65] may often depend on the type of telecommunications device on which they are communicating. For example, the privacy interests in a communication on a speaker-phone in an open office are less than those in a communication on an extension phone in a private office.[66] But an employer must minimize the secrecy of any surveillance in order to conform with the Omnibus Act's "ordinary course of business" exception.[67] Thus, an employer conducting surveillance on an extension, speaker, or other type of phone with reduced privacy must eliminate the surreptitiousness of the surveillance by acquiring the parties' consent, particularly where a communication may be "personal" rather than "busi-

implicitly incorporates the federal participant consent exception into the ordinary course of business exception. *See infra* notes 73-75 and accompanying text.

62. *See* United States v. Christman, 375 F. Supp. 1354, 1355 (N.D. Cal. 1974) (department store's chief of security, suspecting employee involvement in criminal activities, intercepted calls through a specially installed extension phone).

63. Campiti v. Walonis, 611 F.2d 387, 392 (1st Cir. 1979).

64. *See, e.g.*, Briggs v. American Air Filter Co., 630 F.2d 414 (5th Cir. 1980) (surreptitious monitoring of an employee's conversation is permissible if the conversation is business related); James v. Newspaper Agency Corp., 591 F.2d 579 (10th Cir. 1979) (monitoring of business calls to assist employee training within ordinary course of business exception); U.S. v. Harpel, 493 F.2d 346 (10th Cir. 1974) (use of extension phone without any party's consent is not within the ordinary course of business exception). Most states are in accord with this latter principle. *See, e.g.*, Ribas v. Clark, 154 Cal. App. 3d 1007, 696 P.2d 637, 201 Cal. Rptr. 721 (1984).

65. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

66. *See* State v. Tsavaris, 394 So. 2d 418, 420 (Fla. 1980) (detective's testimony regarding a conversation he overheard while listening in on a speaker-phone without the caller's knowledge admissible; however, tape recording held inadmissible).

67. *See infra* notes 73-82 and accompanying text (discussing the contextual approach of analyzing business surveillance).

ness-related."[68]

A phone conversation within the "ordinary course of business exception" may be a business call or, in some limited situations, a personal call. For example, monitoring sales representatives' calls as a means of improving sales techniques is permissible, such calls being business communications.[69] Also, a supervisor may legitimately monitor the conversation of an employee whom he suspects is divulging business secrets to competitors, even though such a call could be termed personal.[70] However, employers may intercept a personal call only to the extent necessary to determine if it is of a business or personal nature.[71] There is some disagreement concerning where the borderline between business and personal calls should be. Courts analyzing this problem generally state that a business call must be "reasonably related to a business purpose."[72] The next section presents an analysis of the methods courts use in addressing these issues.

2. *Case Synopses*

The relatively few cases interpreting the Omnibus Act's ordinary course of business exception fail to take a consistent approach in analyzing the exception. However, a number of cases provide useful insights into the factors courts consider significant in deciding the lawfulness of employers' actions in monitoring or recording communications in the workplace. In these cases, courts primarily take one of two analytical approaches in deciding whether to impose liability for employer surveillance. The context approach focuses on whether the context of the employer's surveillance is proper. The content approach in-

68. *See infra* notes 85-113 and accompanying text.

69. Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983).

70. Briggs v. American Air Filter Co., 630 F.2d 414 (5th Cir. 1980). The court went even further, stating that "[the] interception of calls reasonably suspected to involve non-business matters [is] justifiable [if] the employer has had difficulty controlling the personal use of business equipment through prior warnings." *Id.* at 420 n.8. Judge Thomas A. Clark concurred in the court's judgement except for the statement in footnote 8. Judge Clark stated that a private call, such as the one described in the footnote, could not be intercepted. *Id.* at 421 (Clark, J., concurring).

71. Epps v. St. Mary's Hosp., 802 F.2d 412, 416 (11th Cir. 1986); Watkins v. L.M. Berry & Co., 704 F.2d 577, 583-84 (11th Cir. 1983).

72. Briggs v. American Air Filter Co., 630 F.2d 414, 420 (5th Cir. 1980); James v. Newspaper Agency Corp., 591 F.2d 579, 581-82 (10th Cir. 1979) (installation of monitoring device with notice to employees was for "legitimate business purpose" of training employees and controlling abusive customer phone calls).

quires whether the employer has an interest in acquiring the content of a particular phone communication. The following sections use this taxonomy in presenting a synopsis of the pertinent monitoring and recording cases. Note, however, that a few of the cases include analyses from both the context and content approaches.

a. Context Approach

The context approach emphasizes factors such as whether there are (1) adequate business justifications for the surveillance; (2) proper notification to employees; and (3) congruity between announced procedural safeguards and their actual administration. The general rule is that employers will not be liable for interceptions if they meet a checklist of objective factors.

Use of the context approach to analyze whether a communication is within the ordinary course of business exception is anomalous in one major respect. The exception only applies to wire communications which do not require that speakers have a subjective expectation of privacy. The nonconsensual interception of a wire communication is itself actionable regardless of whether the speakers believed their conversation was private. The context approach, nevertheless, incorporates some elements of the subjective expectation analysis. For example, courts using the context approach consider whether a company gave adequate notice to its employees before surveillance began. Since notice affects employees' subjective expectations of privacy, this factor seems inappropriate in analyzing wire communications. However, courts can justify the use of such factors because the ordinary course of business exception is an exception to the statutory definition of a wire communication.

The seminal case in the area, *United States v. Harpel*,[73] sets the minimum standard for workplace monitoring: employer authorization and adequate notice. *Harpel* involved a criminal prosecution under the Omnibus Act. Harpel was convicted of disclosing a recorded telephone conversation between a police department officer and federal drug agents.[74] There was little evidence regarding who made the recording or how the recording was accomplished. In addition, neither the officer nor the

73. 493 F.2d 346 (10th Cir. 1974).

74. The recordings were played on two separate occasions at a local bar. *Id.* at 348.

federal agents had consented to the recording. The primary issue was whether the "extension phone" exception applied.

Harpel contended that no interception occurred if the recording took place on an extension telephone connected to the police department lines. The court rejected this rigid application of the "extension phone" exception, holding as a matter of law that "a telephone extension used without authorization or consent to surreptitiously record a private telephone conversation is not used within the ordinary course of business."[75] Consequently, a nonconsensual recording on an extension phone of the officers' conversation was an illegal interception, and disclosure of the recording to others was not protected by the statutory exception.

Courts using the context approach tend to stress a business's interests in safeguarding its service quality or preventing unauthorized use of the company phone system. For example, in *James v. Newspaper Agency Corp.*,[76] a former employee of the Newspaper Agency (the Agency) sued under the Omnibus Act, alleging that the Agency had unlawfully intercepted wire communications by installing a telephone monitoring system. The Agency had requested the telephone company to install a monitoring device, which permitted the Agency to listen in on telephone conversations between its employees and its advertisers and others.[77] The Agency was concerned about abusive language by irate customers, and the need to give employees further training and supervision in dealing with the public.[78]

The court, using a contextual approach, noted that the installation was not done surreptitiously. All employees were advised in advance, in writing, of the installation; none protested.[79] The court held that the installation was "squarely within" the ordinary course of business exception.[80] Because the installation was not done secretly, all employees were notified, and the installation was for a legitimate business purpose; the interception was in the ordinary course of business.[81]

Similarly, in *Simmons v. Southwestern Bell Telephone Co.*,[82]

75. *Id.* at 351.
76. 591 F.2d 579 (10th Cir. 1979).
77. *Id.* at 581.
78. *Id.*
79. *Id.*
80. *Id.*
81. *Id.* at 582.
82. 452 F. Supp. 392 (W.D. Okla. 1978), *aff'd*, 611 F.2d 342 (10th Cir. 1979).

the court upheld a telephone company's monitoring of its employees who dealt with telephone complaints and customer inquiries. In this case, however, the court relied on the "common carrier" exception.[83] The company had installed a monitoring system in order to control employees' performance quality, check work in progress, and supervise employees' contacts with the public. The court found significant that in addition to notifying employees about monitoring, the company made unmonitored phones available for employee use.[84]

b. Content Approach

The content approach focuses on the nature of a call's content: "business" calls can be subject to surveillance; "personal" calls cannot. However, this seemingly simple dichotomy has one major problem: the nature of a particular call cannot be ascertained until after it is subject to surveillance. There is no way for the employer to determine before monitoring a call whether it is business or personal.

For example, in *Epps v. St. Mary's Hospital of Athens*,[85] the Eleventh Circuit decided that an employer's use of a recording device did not violate the federal wiretapping statute. Appellants, both hospital employees, engaged in a conversation over a "ringdown line"[86] which connected two telephones, one at the

83. The Omnibus Act actually has two provisions that except wire and electronic communication service providers (termed "common carriers" prior to the Privacy Act amendments). The first exception provides that:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical of service quality control checks.

18 U.S.C. § 2511(2)(a)(i) (1987). The second provision is the "ordinary course of business" exception. It excepts the use of telephone equipment and facilities "used by a communications common carrier in the ordinary course of its business." *Id.* § 2510(5)(a)(i). Florida's common carrier exception is more general than the federal provision. FLA. STAT. ANN. § 934.02(4)(a) (West 1985). It simply recognizes common carriers within the "ordinary course of business" exception. *Id.*

84. 452 F. Supp. at 396.

85. 802 F.2d 412 (11th Cir. 1986).

86. A button at the dispatch station caused the substation telephone to ring; however, the call passed first through Southern Bell's central office before arriving at the substation. Incoming and outgoing calls originating at the dispatch station were auto-

hospital's main dispatch station and the other at a downstairs substation. A third employee in an adjacent room overheard the appellants' conversation, which contained disparaging remarks about two dispatch supervisors. After listening for fifteen minutes, the second employee relieved the dispatcher on duty and began recording the call a few minutes later. The appellants filed suit for actual and punitive damages under the federal wiretapping statute, alleging that other employees listened to and disclosed the contents of the recording.[87]

The appellants argued that the statutory exception did not apply because the interception and recording of the conversation was not in the ordinary course of hospital business. In support of their assertions they demonstrated that: (1) it was hospital policy to record automatically only calls coming into or going out from the dispatch console; (2) hospital personnel were not authorized to record any other calls; and (3) the employee recording the call was not an authorized dispatcher.[88] These factors indicate a contextual approach towards determining liability against the hospital. The hospital, however, argued that the call was in the ordinary course of business because the *content* of the conversation dealt with employee relations, which were of direct concern to the hospital.[89]

In adopting the content approach, the court held that the call was not personal because it occurred during office hours, between co-employees, over a specialized extension, and contained "scurrilous" remarks about supervisory employees in their capacities as supervisors.[90] The court stated that

matically recorded. Calls on the ringdown line were not automatically recorded but could be manually recorded. This distinction would preclude analysis under the "private system" exception, which prevents application of the Omnibus Act's provisions to privately operated in-house telecommunications systems. *See, e.g.*, U.S. v. Christman, 375 F. Supp. 1354, 1355 (N.D. Cal. 1974) (closed dial telephone system used only for calls within store or to other stores of the same chain). *See generally* Note, *supra* note 30, at 451-52 (discussion of private system exception).

87. 802 F.2d at 414.

88. *Id.* at 416.

89. *Id.* The hospital urged that the ringdown line was not a "facility" under the definition of a "wire communication." *Id.* at 414. The court held that the entire phone system, not just the extension line, is a facility under the Omnibus Act; therefore, the conversation was a wire communication. *Id.* at 414-15. The appellants also argued that the double reel recording device was an intercepting device not furnished by a common carrier. *Id.* at 415. The court, however, did not accept this argument. Instead, the court stated that "the intercepting device was the dispatch console. The console intercepted the call. The double reel recorder recorded it." *Id.* at 415.

90. *Id.* at 417.

"[c]ertainly the potential contamination of a working environment is a matter in which the employer has a legal interest."[91] The court concluded that the case fell within the "telephone extension exception;" thus, the hospital was not liable.[92]

In dissent, Judge Phyllis Kravitch disagreed with the majority's analysis because it relied on the content of an employee's conversation to determine whether it was within the ordinary course of business.[93] Judge Kravitch stated that there must be a legitimate business purpose and authorization before an employer may intrude on an employee's privacy; the business purpose must also exist at the time the conversation is recorded.[94]

Judge Kravitch's dissent illustrates a flaw in the content approach: how to determine the nature of a call's contents before surveillance occurs.[95] The dissent's argument supports the use of the contextual approach by urging that certain factors be met. The dissent implicitly raises a second issue as well: should courts decide whether the content of a particular conversation is business or personal after the fact?

The line between personal and business calls is at best amorphous. Some might argue that the majority in *Epps* improperly concluded that an employee's "scurrilous remarks" should be the basis for exempting an employer from wiretap liability, particularly when almost all the factors under the context approach were absent. The court could easily have held that the employee's communication was not business-related, and thus was protected under the Omnibus Act.

The Eleventh Circuit also took the content approach in *Watkins v. L.M. Berry & Co.*[96] Plaintiff Watkins, a sales representative for the Berry Company, solicited advertisements for the Yellow Pages. Part of Berry's established training program involved the monitoring of solicitation calls and reviewing them with employees to improve sales techniques. Monitoring was done with a standard extension telephone. Employees were permitted to make personal calls on company telephones; however, they were told that personal calls would not be monitored except to the extent necessary to determine whether a particu-

91. *Id.*
92. *Id.*
93. *Id.* (Kravitch, J., dissenting).
94. *Id.* at 418.
95. *See infra* notes 96-106 and accompanying text.
96. 704 F.2d 577 (11th Cir. 1983).

lar call was of a personal or business nature.[97]

A friend called Watkins during lunch hour, and Watkins mentioned a job interview she had with another company. The conversation was being monitored by her supervisor, and Watkins was fired. She brought suit against Berry and her supervisor under the federal wiretapping statute.

The court stated the general rule: "[I]f the intercepted call was a business call, then Berry Co.'s monitoring of it was in the ordinary course of business. If it was a personal call, the monitoring was probably, but not certainly, *not* in the ordinary course of business."[98] The court rejected Berry's argument that the monitoring was in the ordinary course of business simply because the contents might be of interest to Berry. Though Berry may have been interested in Watkins' interview and possible employment plans, it was of no legal interest to them: "Her interview was thus a personal matter, neither in pursuit nor to the legal detriment of Berry's business."[99] The court ruled that "a personal call may not be intercepted in the ordinary course of business . . . except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not."[100] In summary, the court stated that "a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents."[101]

The court also discussed two additional issues. First, Berry had intercepted an incoming call, but Berry's business was to place outgoing solicitation calls. The court said that if Berry knew the intercepted call was incoming, the entire listening would have been unlawful.[102] Second, the court addressed the issue of how long Berry could monitor Watkins' call after le-

97. *Id.* at 579.

98. *Id.* at 582 (emphasis in original).

99. *Id.* at 582.

100. *Id.* at 583.

101. *Id.* The court stated that it was making the "positive, affirmative statement" Judge Thomas A. Clark had urged in his concurrence in *Briggs*. However, in *Briggs* Judge Clark proposed a steadfast rule: private calls simply cannot be intercepted. 630 F.2d at 421. The *Watkins* court, therefore, did not adopt Judge Clark's view in its entirety. Instead, it adopted a position substantially in accordance with the majority in *Briggs*, with which Judge Clark took issue. *Cf.* 630 F.2d at 420 n.8.

102. 704 F.2d at 584 n.8. *Cf.* Op. Att'y. Gen. Fla. 85-5 (Jan. 23, 1985) (municipal police department may lawfully record incoming calls to department's lines but may not lawfully record outgoing calls on such lines even if lines are equipped with audible "beeper" signal).

gally entering the conversation. The court noted that the "expectation of privacy in a conversation is not lost entirely because the privacy of part of it is violated."[103] The supervisor "was obliged to cease listening as soon as she had determined that the call was personal, regardless of the contents of the legitimately heard conversation."[104] The court noted that other cases allowing interceptions of ten to fifteen seconds were sensible; however, one case upholding a three to five minute interception was troubling.[105] The limits of the exemption are directly related to the company's policy and are questions for the trier of fact.[106]

In the Fifth Circuit, *Briggs v. American Air Filter Co.*[107] concerned an action brought for invasion of privacy under the Omnibus Act. The manager of American Air Filter suspected that an employee was disclosing confidential information to a former employee who worked for a competing firm. The employee and former employee were friends prior to the conversations at issue. The manager admonished the employee not to discuss any of the company's business with the former employee. However, the manager subsequently received information from various sources that the employee was continuing to discuss contracts with the former employee. Following a confidential discussion of company business with the employee, the manager was told by a secretary that the employee was talking to the former employee on the phone. Both the employee and the manager were in their private offices. The manager picked up his phone, an ordinary extension phone, and recorded part of the conversation.

Both parties stipulated that the call was business-related, though there was disagreement over whether the call contained confidential information. The recording was done with an attachment to a portable dictation machine which was "a standard piece of equipment which had been provided when the dictating machine was purchased."[108] Neither the employee nor the former employee had been informed that their call might be monitored, and neither had consented to being

103. 704 F.2d at 584.

104. *Id.*

105. *Id.* at 584-85. *But see* United States v. Axselle, 604 F.2d 1330, 1335 (10th Cir. 1979) (operator monitoring call for three to five minutes permitted).

106. 704 F.2d at 584-85.

107. 630 F.2d 414 (5th Cir. 1980).

108. *Id.* at 416.

monitored.[109]

American Air Filter counterclaimed for breach of loyalty. The trial court granted summary judgment in defendant's favor and the employee appealed. On appeal, the court said the issue was simply whether the manager's telephone was one that was used in the ordinary course of business. Since the court found it was, it held the telephone was not a "device" under the Omnibus Act.[110] The court, concluding that Congress authorized the interception of this type of communication, made three points. First, the plaintiffs stipulated that the call was a business call. Second, the manager's listening was limited in time, and was for a specific business-related purpose. Thus, the court did not have to address the issue of whether listening would violate the act if the conversation had been "personal."[111] Third, the act of listening was not part of a general practice of surreptitious monitoring. A general practice of listening, the court held, would be more intrusive of employees' privacy than monitoring limited to specific occasions. The court did not reach the issue of whether a general practice of random monitoring of employee calls is justifiable under the Act.[112] The court did note that the practice of listening may violate state law.[113]

c. Content v. Context

The context approach provides clearer guidelines for employers than the content approach. By complying with the factors highlighted in the cases above, employers can be certain that their surveillance systems will not run afoul of the "ordinary course of business" exception.

---

109. *Id.*

110. *Id.* at 417.

111. *Id.* at 420. However, in a footnote the majority indicated the difficulty it had envisioning situations where the interception of non-business calls would be permissible. The majority then stated: "However, interception of calls reasonably suspected to involve non-business matters might be justifiable by an employer who had difficulty controlling personal use of business equipment through warnings." *Id.* at 420 n.8. Judge Thomas A. Clark, specially concurring, disagreed. He proposed a rule that monitoring of personal calls would be impermissible, even under the majority's hypothetical. *Id.* at 421 (Clark, J., concurring). *See supra* note 101 for a further discussion of this issue.

112. *Id.* at 420; *but see* James v. Newspaper Agency Corp., 591 F.2d 579 (10th Cir. 1979) (monitoring of employee phone calls by supervisors was within the extension phone exception) discussed *supra* notes 76-81 and accompanying text.

113. 630 F.2d at 420.

However, there may be situations where, despite compliance with the context approach's checklist, employers will monitor or record a "personal" call. For instance, an employer with a legitimate business purpose and actual employee notice might monitor a personal phone call on a "business-only" phone. Under the context approach, the employer's monitoring would not be actionable. But, under the content approach, the employee could argue that the employer had no justifiable interest in monitoring the contents of the call.

While the content approach would at first glance appear to favor the privacy rights of employees, it may actually favor employers under the proper circumstances. For example, in both *Briggs* and *Epps* the court determined that the employers had an interest in the content of their employee's conversation. The courts labeled the calls "business" and upheld the employers' activities. A contextual approach would have reached a different result because the businesses in both cases had failed to meet procedural prerequisites, such as notice to employees. Courts' use of the content approach is thus a two-edged sword. The content approach may override the context approach in situations where employers, although complying with procedural safeguards, overstep and invade employees' private communications. It can also favor employees, however, as evidenced by the *Epps* and *Briggs* decisions.

3. *Participant Consent Exception*

Consent is a consideration independent of interception under the Omnibus Act.[114] The Omnibus Act exempts the interception of wire, oral or electronic communications if (1) the person intercepting the communication is a party to the communication, or (2) one of the parties to the communication has given prior consent to such interception.[115] Therefore, recording or

114. United States v. Harpel, 493 F.2d 346, 350 (10th Cir. 1974). The holding in *Harpel* is peculiar because, although the court states that consent is a consideration independent of interception, the court actually incorporates consent into the ordinary course of business exception (which is within the definition of interception). In other words, the consent exception does not require that a communication be "in the ordinary course of business;" however, for a communication to be "within the ordinary course of business" there must be the consent of at least one party.

115. 18 U.S.C. § 2511(2)(d) (1987) provides:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such com-

monitoring one's own communications is permissible without the consent of the other parties to the conversation.[116]

Simply taping a telephone conversation does not violate the Omnibus Act, provided at least one party consents.[117] Congress intended to permit one party to record conversations with another when the recorder is acting out of a legitimate desire to protect himself[118] by having an accurate recording of conversations to which he is a party.[119] An interception is illegal if done for the purpose of committing any criminal or tortious act, even if the interceptor meets one of the participant consent exceptions.[120]

In the business context, employers may seek to avoid liability under the Omnibus Act by having employees consent to monitoring. Because of the current emphasis on privacy interests, courts are hesitant to find actual or implied consent unless the circumstances clearly indicate that employees were adequately warned that their communications might be monitored or recorded. Accordingly, careful planning and implementation of a company policy are necessary to achieve effective employee consent.

---

munication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

Id.

116. *See, e.g.*, United States v. Viviano, 437 F.2d 295, 300 (2d Cir. 1971) (tape recording with consent of a party to conversation does not violate Omnibus Act or fourth amendment); Consumer Elec. Prods. v. Sanyo Elec., 568 F. Supp. 1194, 1196 (D. Colo. 1983); Smith v. Wunker, 356 F. Supp. 44, 46 (S.D. Ohio 1972) (recording of private telephone conversation by a party to it and its subsequent disclosure did not violate Omnibus Act).

117. Consumer Elec. Prods. v. Sanyo Elec., 568 F. Supp. 1194, 1197 (D. Colo. 1983) (noting that the burden of proof is on the party alleging an interception to show an unlawful purpose). *See also* United States v. W. Phillips, 540 F.2d 319, 326 (8th Cir. 1976) (placing burden on party making interception to prove that interception was not for unlawful purpose creates an "impossible burden" of proving negatives). *But see infra* notes 188-97 and accompanying text (Florida state law requires that all parties consent).

118. *See* 114 CONG. REC. 14,694 (1968) (Statement of Sen. Hart).

119. By-Prod Corp. v. Armen-Berry Co., 668 F.2d 956, 959-60 (7th Cir. 1982). *See also* Moore v. Telfon Comm. Corp., 589 F.2d 959, 965-66 (9th Cir. 1978) (holding that Omnibus Act does not prohibit franchiser's recording of conversation with franchisee for the purpose of preserving evidence of extortion for later use to support termination of franchisee).

120. 18 U.S.C. § 2511(2)(d) (1982). This provision modifies the original version, which exempted all wire and oral communications from the Omnibus Act where one party consented. S. REP. NO. 1097, 90th Cong., 2d Sess., *reprinted in* 1968 U.S. CODE CONG. & ADMIN. NEWS 2112, 2182.

In *Watkins v. L.M. Berry & Co.*,[121] Watkins filed suit after her employer monitored a personal call on a company phone. Employees were permitted to make calls on company telephones, and they were told that calls would only be monitored to the extent necessary to determine whether it was personal or business. In its defense, the employer urged that the participant consent exception applied because plaintiff's acceptance of employment with knowledge of the established monitoring policy constituted consent to the interception of the call.

The court found this argument erroneous with respect to both actual and implied consent theories. The court stated:

> It is clear, to start with, that Watkins did not actually consent to interception of *this* particular call. Furthermore, she did not consent to a *policy* of general monitoring. She consented to a policy of monitoring sales calls but not personal calls. This consent included the inadvertent interception of a personal call, but only for as long as necessary to determine the nature of the call.[122]

The court also declared that under the Omnibus Act "knowledge of the *capability* of monitoring alone cannot be considered implied consent."[123] The court distinguished the situation here from two others. First, courts will imply consent where the plaintiff knew or should have known of a policy of *constantly* taping calls.[124] Second, courts will imply consent where a personal call is made on a telephone which the employee knows is to be used exclusively for business calls and is regularly monitored.[125] Here, by contrast, the plaintiff consented only to limited monitoring of business calls.

---

121. 704 F.2d 577 (11th Cir. 1983). *See also supra* notes 96-106 and accompanying text (further discussion of *Watkins*).

122. 704 F.2d at 581 (emphasis in original).

123. *Id.* (emphasis in original). *See also* Campiti v. Walonis, 611 F.2d 387 (1st Cir. 1979). A prisoner whose phone conversation had been monitored argued that he had not given prior consent. The defendants urged that the prisoner had given implied consent because (1) the prisoner was in restricted custody, (2) the call was placed by a staff officer, (3) the common practice in the prison was to monitor inmate calls, and (4) inmates' general expectations are that calls are monitored. *Id.* at 393. However, the court held that the defendant's theory "completely distorted" the plain words of section 2511(2)(c), which requires prior consent. *Id.* at 394.

124. 704 F.2d at 581. *See, e.g.*, Jandak v. Village of Brookfield, 520 F. Supp. 815 (N.D. Ill. 1981) (police officer whose call was intercepted knew or should have known that the line he used was constantly taped for police purposes).

125. 704 F.2d at 581-82. *See, e.g.*, Simmons v. Southwestern Bell Tel. Co., 452 F. Supp. 392 (W.D. Okla. 1978), *aff'd*, 611 F.2d 342 (10th Cir. 1979) (plaintiff made personal call on phones designated for business use, after previously being warned, even though other phones were specifically provided for personal use).

The Omnibus Act does not grant non-employee callers any right to notification that their communications are subject to monitoring.[126] As long as one party consents, the participant consent exception applies.[127] In essence, participant consent is unilateral so the receiver may monitor calls without the caller's knowledge.[128] This aspect of the Omnibus Act has led to various proposals such as special designations in phone books[129] and state rules requiring the consent of all parties.[130] However, no federal standard has emerged.[131]

One suggestion for dealing with the employee and customer notice problem is for employers that monitor workplace telephones to use an audible periodic warning tone. Congress is currently considering a so-called "beeper bill" that would amend the Omnibus Act by implementing this type of protection. The bill provides:

> "Notwithstanding any other provision in the chapter, it shall be unlawful for an employer (or an agent of an employer) to listen in on an employee's work phone call unless a repeating audible tone is utilized to warn parties to the call. Any person whose call is listened in on in violation of this subsection may recover civil damages as provided in section 2520 for an interception of communications in violation of this chapter.[132]

The bill has enormous implications. First, the bill's proviso requires that it override any conflicting provisions in the Omnibus Act. For example, even if an intercepted communication was "within the ordinary course of business," the employer

126. When *recording* is involved, however, FCC rules and phone company tariffs require all party consent or beep-tones. *See infra* notes 145-54 and accompanying text.

127. Of course, an employer who fails to notify an employee that a phone is subject to monitoring may be sued by both the employee and the individual calling the employee. *See* Awbrey v. Great Atl. & Pac. Tea Co., 505 F. Supp. 604, 606-07 (N.D. Ga. 1980).

128. This application of the participant consent provision, however, is symmetrical. A caller may monitor his own call to a business or government agency without notifying the business or agency.

129. *See* Electronic Surveillance, Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance 28 (1976) (suggesting the FCC or state utility commissions consider requiring asterisks beside names of companies engaging in service monitoring).

130. *See infra* notes 188-97 and accompanying text.

131. This lack of uniformity is a considerable concern for those who sell nationally by telephone. *See* Higgins, *To Tape or Not to Tape is Question for Telemarketers*, Marketing News, May 9, 1986, at 4 (telephone service representatives in legal limbo).

132. H.R. 1950, 100th Cong., 1st Sess. (1987); S. 1124, 100th Cong., 1st Sess. (1987). The bills are identical.

would still have to use a beep-tone device. Similarly, the bill would override the participant consent exception even if *all* parties consented to the interception. Thus, the bill would effectively make much of the existing case law irrelevant.[133]

Furthermore, the employer would be liable for civil damages not only to employee-parties but to any other parties to the call.[134] The bill expands privacy protection to all parties and resolves any ambiguities regarding whether an employer is liable to non-employees for workplace violations.[135] Also, the bill is more expansive than current FCC regulations, which require a beep-tone only when recording activities take place.[136] Finally, the bill applies only to work phone calls; personal phone calls are not included. This language could cause problems in those situations where a workplace phone is used for both business and personal calls. For example, suppose an employee uses a workplace phone for a personal call and the beep-tone continues to chime. Is the employer liable for monitoring the call or is the employee implicitly consenting to the possible monitoring?[137]

The beep-tone might also detrimentally affect a speaker's candor, brevity, and informality while reducing precision and lucidity of thought.[138] A continual beep may also make customers feel uncomfortable or suspicious.[139] In addition, the bill might increase the operational costs of those employers who continued to monitor workplace telephone communications.

4. *Privacy Interests — Generally*

A recurrent theme throughout the Omnibus Act case law is the protection of privacy interests. This section highlights the

133. The monitoring and recording activities that courts upheld as being within the ordinary course of business exceptions in the *Newspaper Agency*, *Simmons*, *Epps*, and *Briggs* cases would be impermissible under the bill's provisions because the employer did not use an audible beep tone.

134. *Id.*

135. The bill limits liability to "civil damages as provided in section 2520 for an interception of communications in violation of this chapter." *Id.* This section provides for recovery of damages (statutory, actual, and punitive), attorneys' fees and litigation costs.

136. *See infra* note 147 and accompanying text. The bill refers to "listening in" activities, which are much broader than just "recording." *See infra* notes 145-54 and accompanying text.

137. This could be a particularly difficult problem when employers use automated equipment which cannot distinguish between business and personal calls.

138. *See* R. Posner, *supra* note 2, at 245-47.

139. *See* Higgins, *supra* note 131, at 4.

methods of determining what constitutes an expectation of privacy under the Omnibus Act.

Wire and electronic communications (telephone communications), unlike oral communications, are protected against interceptions by electronic, mechanical, and other devices regardless of the speaker's expectation of privacy.[140] Thus a speaker's privacy expectations would seem irrelevant in determining whether a particular interception of a telephone communication is justifiable. However, privacy expectations are relevant in determining whether a communication is within the "ordinary course of business" exception (content approach), and in looking at state tort law, which is examined in Part II of this article.[141]

In monitoring or recording telephone conversations, an employer should take the greatest care not to tortiously invade the privacy of one of the parties. One party may have a legitimate expectation of privacy so that the interception, use or disclosure of the conversation is actionable under the Omnibus Act or state tort law. What constitutes a legitimate expectation of privacy is unclear. For example, one federal court stated that each willing participant in a conversation takes the risk that another participant may divulge the contents of the conversation; if the conversation is divulged, either by memory of the participant or by electronic reproduction, there is no violation of any privacy right.[142]

Both subjective and objective expectations of privacy determine whether an expectation of privacy is justified. This two-part test is referred to in *Katz v. U.S.*,[143] which discusses what constitutes an "oral communication" under the Omnibus Act. The subjective expectation relates to whether a person's conduct exhibits an actual expectation of privacy;[144] the objective standard inquires whether a person's subjective expectation is one which society is prepared to recognize as reasonable.[145]

---

140. *See supra* note 38 and accompanying text.

141. *See infra* notes 154-212 and accompanying text.

142. United States v. W. Phillips, 540 F.2d 319, 324-25 (8th Cir. 1976), *cert. denied*, 429 U.S. 1000 (1977).

143. 389 U.S. 347 (1967).

144. *Id.* at 361 (Harlan, J. concurring).

145. *Id. See also* State v. Inciarrano, 473 So. 2d 1272, 1275 (Fla. 1985) (homicide defendant had no reasonable expectation of privacy, so the deceased's recording of conversation and his own death was not in violation of Security of Communications Act).

Employers can directly affect the subjective expectations part of the test. For example, an employer notifying employees that phone communications are to be monitored or recorded essentially minimizes any subjective expectation of privacy employees may have. However, a person's subjective expectation of privacy in, for example, direct oral communications with other employees is much different. In this situation, the employee expects the conversation to be private; eavesdropping on this type of oral communication would probably violate the Omnibus Act and state privacy laws.[146] In fact, interception of the same conversation occurring over a telephone line would be unlawful unless the extension phone, ordinary course of business, or consent exceptions applied.

Employers can also affect the objective standard, because it is based on the reasonableness of the employee's subjective expectation. However, other extrinsic factors over which an employer has little control affect the reasonableness test. For example, courts use factors such as the location and volume of a conversation to determine reasonableness.[147]

B. Federal Communications Commission Orders

The FCC's orders and regulations provide another hurdle to employers' recording of employees' business-related conversations. FCC orders are applied to the general public through tariff provisions[148] which make individual telephone companies responsible for enforcing the Commission's rules against their customers. For example, telephone companies subject to the Commission's jurisdiction may terminate the telecommunications services of customers using recording devices in noncompliance with Commission rules. A business's failure to comply with telephone company warnings may result in the suspension of the business's telecommunications service until the customer complies with the tariff's provisions. [149] A telephone company

146. 389 U.S. at 352-53.

147. *See* cases cited in Note, *supra* note 30, at 444 n.39. Changing technology also affects the expectation of privacy. *Id.* at 445-46.

148. FCC recording regulations are applied to telephone companies themselves by Commission rule. *See* 47 C.F.R. § 64.501 (1987).

149. However, some courts have held, in the criminal context, that Commission orders requiring a beep-tone are directed to telephone companies, not their customers. Ferguson v. U.S., 307 F.2d 787, 790 (10th Cir. 1962) (course of federal prosecution cannot be controlled by state law), *opinion withdrawn on other grounds per curiam*, 329 F. Supp. 611, 615 (D.Minn. 1973) (FCC beep-tone order contrary to Congres-

that fails to enforce its tariffs could be subject to fines or the amendment, suspension, or revocation of its service certificates.

The Commission promulgated its first rule regulating the recording of phone conversations in 1947.[150] The Commission adopted the rule to balance the legitimate public needs for recording phone communications and the protection of individual privacy interests. Recording of two-way telephone conversations over interstate or wide area telecommunications services was permissible provided the recording party used a beep-tone at periodic intervals to protect the privacy of telephone communications.[151]

Four years later, in 1951, the Commission became concerned that recording was being done with devices over which phone companies and the Commission had little control. The Commission prohibited the recording of phone messages by acoustic or inductive methods. Only the telephone companies could make connections for recording calls because interconnection of "foreign" attachments was prohibited by tariff.[152] In 1981, the Commission adopted mutual consent as a substitute, not a replacement, for the beep-tone requirement.[153] If all parties to a telephone conversation consent to recording of the communication, a beep-tone is not necessary.[154]

The Commission has continued to protect privacy interests in telephone communications. However, the most recent Commission order provides a third option: recording is permitted if the recording party notifies the other party that it intends to record the conversation.[155] Notice should be made at the beginning, and as part of, the recorded portion of any call.[156] This

---

sionally-enacted exceptions). This rationale suggests the maximum sanction businesses not complying with FCC orders may be subject to is termination of their telecommunications services.

150. Use of Recording Devices, Report and Order, 11 F.C.C. 1033 (1947).

151. *Id.* at 1055, para. 3.

152. However, such tariff provisions are suspect following the 1968 Carterfone decision in which tariffs restricting attachment of non-telephone company equipment were found unlawful. Use of the Carterfone Device in Message Toll Telephone Service, 13 F.C.C.2d 420 (1968), *reconsideration denied*, Memorandum Opinion and Order, 14 F.C.C.2d 571 (1968).

153. Recording Devices, Memorandum Opinion and Order, 95 F.C.C.2d 848 (1983).

154. The Commission also identified three types of calls that may be recorded without a beep-tone or consent: emergency, patently unlawful, and law-enforcement related. *Id.* at paras. 8-11.

155. Use of Recording Devices in Connection with Telephone Service, Report and Order, 2 F.C.C. Rcd. 502 (1987).

156. For example, suppose a caller informs a receiver that the caller intends to

option still requires all-party consent, but it does allow "implied consent." For example, if after notification a receiver continues to communicate over the phone, the caller may record the conversation.

The FCC's order raises the jurisdictional issue of whether the Commission is authorized to regulate this subject matter. The Commission concluded in its order that Congress, in enacting the Omnibus Act, did not intend to limit the Commission's jurisdiction over regulation in this area.[157] Reasoning that the Omnibus Act was primarily concerned with law enforcement and other interests rather than privacy interests, the Commission ruled that it was authorized to protect privacy interests of telephone users.[158] There is no conflict between the Act and the FCC rules since the privacy interests the Commission seeks to protect are different from those the Omnibus Act protects.

The Commission seems motivated to protect the privacy interests of phone users on both ends of a communication even in the case where, for example, a business simply uses a recordation internally to improve its services to consumers. Essentially, the FCC wants any party whose telephone communication might be recorded to have consented or been given adequate prior notice. This position places one individual's privacy interests paramount to all other individuals' interests in all situations. However, it provides an additional, albeit somewhat ineffectual, safeguard over privacy interests in personal and business communications.

II
State Law: The Florida Experience

Many states have piggybacked on the federal Omnibus Act by enacting their own "little" Omnibus Acts, sometimes adopting the Omnibus Act's language verbatim.[159] Florida's experi-

record their phone conversation. The receiver does not consent but continues to communicate over the phone. Under the mutual consent requirement, the caller could not record the conversation. However, under the new option, the caller has satisfied the notice requirement and may record the conversation. The receiver has impliedly consented to recordation. However, the option requires that notice be made "as a part of" the recorded portions of the call. So, the caller is under a continuing duty to notify the receiver throughout the conversation that recording is occurring.

157. *Id.* at para. 19.

158. *Id.*

159. *See* ALASKA STAT. ANN. §§ 42.20.300 to -.340 (1962 & Supp. 1987); ARIZ. REV. STAT. ANN. §§ 13-3001 to -3014 (West 1978 & Supp. 1987); ARK. STAT. ANN. §§ 41-4501

ence is illustrative for a number of reasons. First, Florida has protected individual rights on wiretap privacy issues, since its constitution explicitly recognizes a right of privacy[160] and a right to be free from unreasonable search and seizure (including interceptions of private communications).[161] Second, Florida's wiretapping statute parallels the Omnibus Act to a great

---

to -4509 (Supp. 1985); CAL. PENAL CODE §§ 630 -637.5 (West 1985 & Supp. 1988); COL. REV. STAT. ANN. §§ 16-15-101 to -104 (1986); CONN. GEN. STAT. ANN. §§ 54-41a to -41t (West 1985 & Supp. 1987); DEL. CODE ANN. tit. 11, § 1336 (1979 & Supp. 1986); FLA. STAT. ANN. §§ 934.01-.10 (West Supp. 1987); LA. REV. STAT. ANN. §§ 1301-1312 (West 1983 & Supp. 1987); ME. REV. STAT. ANN. tit. 15, §§ 709-712 (1980 & Supp. 1987); MD. CTS. & JUD. PROC. CODE ANN. §§ 10-401 to -411 (1984 & Supp. 1987); MASS. ANN. LAWS ch. 272, § 99 (West 1980 & Supp. 1987); MICH. COMP. LAWS ANN. §§ 750.539a-i (West Supp. 1987); MINN. STAT. ANN. §§ 626A.01-.23 (West 1983 & Supp. 1988); NEB. REV. STAT. §§ 86-701 to -712 (1981); NEV. REV. STAT. §§ 179.410-.515 (1979); N.H. REV. STAT. ANN. §§ 570-A-1 to -11 (1974 & Supp. 1985); N.J. REV. STAT. §§ 156A-1 to -26 (1985 & Supp. 1987); OHIO REV. CODE ANN. §§ 2933.51-.66 (Baldwin 1987); OKLA. STAT. ANN. tit. 13, § 176.2-.14 (West 1983 & Supp. 1987); PA. CONS. STAT. ANN. §§ 5701-5726 (Purdon 1983 & Supp. 1987); R.I. GEN. LAWS § 12-5.1-1 (Supp. 1987); S.D. COMP. LAWS ANN. §§ 23A-35A-1 to -21 (1987 Supp.); TEXAS CODE CRIM. PROC. ANN. art. 18.20 (Vernon Supp. 1987); UTAH CODE ANN. §§ 77-23a-1 to -11 (1978); VA. CODE §§ 19.2-61 to -70 (1983 & Supp. 1987); WASH. REV. CODE ANN. §§ 9.73.030-.100 (1977 & Supp. 1987); W. VA. CODE §§ 62-1D-1 to -16 (Supp. 1987); WISC. STAT. ANN. §§ 968.27-.33 (West 1985); WYO. STAT. ANN. §§ 7-3-601 to -611 (1987).

Some states have provisions that explicitly protect privacy rights in personal communications. *See* ALA. CODE §§ 13A-11-30 to -31 (1975 & Supp. 1986) (defamation and criminal eavesdrop as offenses against privacy); DEL. CODE ANN. tit. 11 § 1335 (1979 & Supp. 1986) (violation of privacy); GA. CODE ANN. §§ 3001-3010 (1983 & Supp. 1987) (unlawful eavesdropping and surveillance); IOWA CODE ANN. § 727.8 (West 1979) (electronic and mechanical eavesdropping violate citizens' health, safety and welfare); KY. REV. STAT. ANN. §§ 526-010 to -.080 (Baldwin 1984) (eavesdropping and related offenses); MONT. CODE ANN. § 5-8-213 (1987) (privacy in communications); N.M. STAT. ANN. §§ 30-12-1 to -11 (1984) (abuse of privacy); N.Y. PENAL LAW §§ 250.00-.35 (McKinney 1984) (offenses against right of privacy); N.D. CENT. CODE ANN. §§ 12.1-15-.02 to .04 (1985 & Supp. 1987) (defamation & interception of communications); S.C. CODE ANN. § 16-17-470 (1976 & Supp. 1986) (eavesdropping).

Finally, a few states have provisions that prohibit the physical intrusion into a wire. ILL. REV. STAT. ch. 134, §§ 15a, 16 (1986 & Supp. 1987) (interference with wire messages and wiretaps, respectively); N.C. GEN. STAT. § 14-155 (1986) (ten dollar daily fine for unauthorized connection with telephone or telegraph); TENN. CODE ANN. § 39-3-1324 (1982) (wiretapping).

160. FLA. CONST. art. I, § 23 provides:

> Right of Privacy. Every natural person has the right to be let alone and free from governmental intrusion into his private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.

Id.

161. FLA. CONST. art. I, § 12 provides, in pertinent part, that "the right of the people to be secure in their persons, houses, papers and effects against the unreasonable searches and seizures, and against unreasonable interception of private communications by any means, shall not be violated."

degree. However, the Florida statute has a few significant differences, notably the two-party consent requirement.

A. Florida Constitution

Some state constitutions contain provisions relating to individual privacy rights.[162] For example, the Florida Constitution creates an individual right of privacy, stating that "[e]very natural person has the right to be let alone and free from governmental intrusion into his private life."[163] This provision, however, relates to interferences by public as opposed to private actors. In addition, the provision applies only to "natural persons," so corporations do not possess the right. One commentator has speculated that the constitutional right extends to "individual" activities but not "economic" activities.[164]

---

162. State constitutions create various types of privacy rights. The first category is a general free-standing right of privacy. *See, e.g.*, ALASKA CONST. art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed upon."); ARIZ. CONST. art. II, § 8 (1982) ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); CALIF. CONST. art. I, § 1 (1972) ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, possessing and protecting property, and pursuing and attaining safety, happiness and privacy."); FLA. CONST. art. I § 23 (1970) (*see supra* note 160); HAWAII CONST. art. I, § 6 (1985) ("The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest."); MONT. CONST. art II, § 10 (1985) ("The right of the individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."); WASH. CONST. art. I, § 7 (1966) ("No person shall be disturbed in his private affairs, or have his home invaded, without authority of law.").

A second category is a right of privacy against unreasonable searches and seizures. *See, e.g.*, ILL. CONST. art. I, § 6 (1986) ("The people shall have the right to be secure in their persons, houses, papers, and other possessions against unreasonable searches, seizures, invasion of privacy, or interceptions of communications by eavesdropping devices or other means."); LA. CONST. art. I, § 5 (1975) ("Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy."); S.C. CONST. art. I, § 10 (1971) ("The right of the people to be secure in their houses, persons, papers, and offices against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated.").

Various state statutes provide for protecting general privacy rights. *See, e.g.*, MICH. STAT. ANN. § 17.62(7) (Callaghan 1982) ("An employer shall not gather or keep a record of employee's associations, political activities, publications, or communications of non-employment activity unless authorized by the employee, unless they occur on the employer's premises, or during working hours, and disrupt the duties of the employee or other employees.").

163. *Id.* § 23. During November 1980, Florida citizens passed this constitutional amendment, which became effective in 1981 by a 60% vote. Note, *Interpreting Florida's New Constitutional Right of Privacy*, 33 U. FLA. L. REV. 565, 565 n.1 (1981).

164. *See* Cope, *To Be Let Alone: Florida's Proposed Right of Privacy*, 6 FLA. ST. U.L. REV. 671, 742 (1978). *But see* Note, *supra* note 155, at 572.

The Florida Constitution also prohibits "unreasonable interception of private communications by any means."[165] Because this additional protection requires state action, its application in the civil area is minimal.[166] However, this provision, as well as the right of privacy provision, is important for their messages: Florida has decided to explicitly protect private communications and individual privacy rights from unreasonable or unnecessary governmental interferences. But the protections afforded private communications from interferences, whether reasonable or not, by private actors have not been elevated to this constitutional level.

B. Florida's Security of Communications Act

Florida's Security of Communications Act[167] parallels the Omnibus Act to a great extent.[168] It similarly prohibits the interception, use, and disclosure of any wire or oral communication.[169] Unlike the Omnibus Act, however, the Florida Act requires all-party consent.[170] The Florida Act also creates a civil cause of action allowing the recovery of actual and punitive damages and attorney's fees.[171] These two provisions dramatically increase the protections available to an individual whose communication is intercepted.

1. *Federal Preemption*

In Florida, courts have held that the Omnibus Act preempts the wiretapping field, so that any state regulation must provide safeguards at least as stringent as those set out in the Act.[172] These cases are consistent with congressional intent.[173]

---

165. FLA. CONST. art. I, § 12. *See supra* note 162 (complete clause).

166. At the time this article was written, only one case dealt with the telephone communications clause. Yarbrough v. State, 473 So. 2d 766 (Fla. Dist. Ct. App. 1985), held that a defendant did not have a reasonable expectation of privacy regarding numbers dialed into a commercial telephone system.

167. FLA. STAT. ANN. §§ 934.01 to .10 (West 1985).

168. *See* Appendix, Diagram 2.

169. FLA. STAT. ANN. § 934.03(1) (West 1985). Unlike in the Omnibus Act, "electronic communications" are not expressly included. *Cf.* Omnibus Act, *supra* note 39.

170. FLA. STAT. ANN. § 934.03 (West 1985).

171. *Id.* § 934.10. Minimum recovery of actual damages is computed at $100 per day or $1,000 per incident, whichever is greater. *Id.* at 934.10(1).

172. State v. Aurilio, 366 So. 2d 71 (Fla. Dist. Ct. App. 1978); State v. McGillicuddy, 342 So. 2d 567 (Fla. Dist. Ct. App. 1977).

173. *See* S. REP. NO. 1097, 90th Cong., 2d Sess., *reprinted in* 1968 U.S. CODE CONG. & ADMIN. NEWS. 2181.

Presumably, Florida could more narrowly construe the extension phone and ordinary course of business exceptions than have federal courts. In fact, one court has held that those portions of Florida's Act authorizing the interception of wire or oral communications are statutory exceptions to the federal and state constitutional right of privacy, and as such, must be strictly construed.[174] The Florida Act's participant consent exception is the best example of a state provision more stringent than the Omnibus Act.

2. *Ordinary Course of Business Exception*

The Florida Act contains an ordinary course of business exception similar to that in the Omnibus Act.[175] As in the federal statute, the exception is embedded in the definition of interception devices.[176] If the requirements of the statutory exception are met, the device in question is not an intercepting device and no violation occurs.

a. Case Law

In *Lomelo v. Schultz*,[177] the plaintiff sued over the defendant's disclosure of a taped telephone conversation. The trial judge dismissed the action based upon the defendant's argument that a wrongful disclosure action cannot be based upon a recording where one party consents. The appellate court reversed, stating that while taping one's own telephone conversa-

174. Copeland v. State, 435 So. 2d 842 (Fla. Dist. Ct. App. 1983), *review denied*, 443 So. 2d 980 (Fla. 1983). An interesting issue is whether an employee could successfully pursue an invasion of privacy tort theory even though a workplace communication is determined to be within the ordinary course of business exception contained in the Florida Act. The issue, reframed, might inquire whether the Florida Act supersedes existing tort law or provides protection equal to or greater than existing tort law. However, the intent element may vary between tort and statutory law. No case law addresses these issues.

175. FLA. STAT. ANN. § 934.02(4)(a) (1985).

176. An "electronic, mechanical, or other device" means

> any device or apparatus which can be used to intercept a wire or oral communication other than: (a) Any telephone or telegraph instrument, equipment, or facility or any component thereof furnished to the subscriber or user by a communications common carrier in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business, or being used by a communications common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties.

Id.

177. 422 So. 2d 1050 (Fla. Dist. Ct. App. 1982)

tion may not be a violation of the statute,[178] playing the tapes to other persons gave rise to a cause of action. Thus, a business may internally use lawfully recorded communications, but the external release of such recordings may violate the disclosure provisions of the Florida Act or constitute an invasion of privacy.

Aside from *Lomelo*, very few civil actions have been brought in Florida under the extension phone and ordinary course of business exceptions. However, the principles Florida courts have enunciated in criminal cases may extend to civil cases as well.

The ordinary course of business exclusion in Florida's wiretapping statute was applied in *State v. Nova*,[179] where a defendant charged with homicide sought to exclude the testimony of the victim's work supervisor.[180] The supervisor listened to a phone conversation between the defendant and the victim-employee following a telephone call earlier that same day from the defendant which had left the victim-employee visibly upset.[181] The trial court concluded that the supervisor was acting in her capacity as supervisor when she listened to the second call. The supervisor had acquired the consent of the victim-employee, and the call was received on a company telephone. Thus, the court found that it was reasonable for the supervisor to listen on the extension phone in order to find out why the victim-employee was so upset. The supervisor's use of the phone was for the benefit of her employee and was in the ordinary course of business.[182] The supervisor's testimony was admissible under the "ordinary course of business" exclusion.[183]

This interpretation of the Florida Acts' "ordinary course of business" exception is different from federal courts' interpreta-

178. Since taping one's own conversations could violate Florida's all-party consent requirement, the court presumably inferred that each party had given consent.

179. 361 So. 2d 411 (Fla. 1978).

180. Exclusion was sought pursuant to FLA. STAT. ANN. § 934.06 (West 1985), which prohibits the use as evidence of intercepted wire or oral communications. The determinative issue in the instant case was whether the "ordinary course of business" exclusion in FLA. STAT. ANN. § 934.02(4)(a) was applicable. 361 So.2d at 413.

181. 361 So. 2d at 413.

182. *Id.* This finding was contradictory to the District Court's determination that the supervisor was merely satisfying her curiosity when she decided to listen in. *Id.* The Supervisor, who found it "funny" that the 53-year-old defendant would constantly call the 22-year-old victim-employee, had even stated "I just wanted to know who was calling her." *Id.*

183. *Id.*

tions of the Omnibus Act's similar provision. First, the supervisor's act of listening was not part of a company monitoring policy. It was an independent act similar to that in *Briggs*. While in *Briggs*, neither party to the conversation had given consent to the recording, here, the employee consented to monitoring of the call. Thus, consent would seem to be the dispositive point. Second, the court relied on the purpose for which the "interception" was made (i.e. for the benefit of the employer) to decide the call was in the ordinary course of business. This factor supports the use of monitoring or recording as a means of furthering legitimate business purposes such as those described in the *Epps* and *Briggs* cases.

In *State v. Tsavaris*,[184] the court held that there was no "interception" within the meaning of the Florida Act when a detective listened to a telephone conversation on a speaker phone without the knowledge of the caller.[185] However, the court held that recording a phone conversation without the consent of all parties is prohibited.[186]

The court's analysis is primarily contextual because it focuses on the type of equipment used and the consent of the receiver. However, undue emphasis on the type of equipment used, rather than on the privacy interests involved, is misplaced.[187]

In *Horn v. State*,[188] the testimony of a nurse's aide who had listened in on a phone conversation between a nurse and her husband was inadmissible in the criminal prosecution of the husband for his wife's murder.[189] Neither of the parties consented, and there was no authority from the nursing home to engage in phone monitoring.[190] The court stated the general rule that all such unauthorized interceptions on extension phones are criminal violations.[191] The court's analysis was

184. 382 So. 2d 56 (Fla. Dist. Ct. App. 1980), *review denied*, 424 So. 2d 763 (Fla. 1983).

185. 394 So. 2d at 420.

186. *Id.* at 421.

187. *See, e.g.*, Campiti v. Walonis, 611 F.2d 387, 392 (1st Cir. 1979).

188. 298 So. 2d 194 (Fla. Dist. Ct. App. 1974).

189. *Id.* The aide admitted being "nosey" when she lifted an extension receiver to listen to the call without the parties' knowledge.

190. *Id.* at 196-97. *See also* Arizona v. Dwyer, 585 P.2d 900 (Ariz. Ct. App. 1978) (a telephone operator who listened to a conversation between the defendant and victim for 15 minutes due to curiosity was not acting within the ordinary course of business).

191. The court revealed the target of its dicta, stating: "It may well have been that in the less complicated era of days gone by party-line eavesdropping furnished an acceptable method of entertainment for bored housewives and others lacking in suffi-

purely contextual because it relied on a steadfast rule requiring at least one party's knowledge and notice of the monitoring.

However, a content approach would support admission of the nurse's aide's testimony.[192] Under the *Nova* and *Epps* rationales, the employer in *Horn* would certainly have an interest in monitoring the type of call here. If a business has an interest in preventing "scurrilous" remarks in the workplace, it would seem to have an interest in preventing or later solving the murder of one of its employees. However, the primary factor that distinguishes *Horn* from *Nova* and *Epps* is the lack of any evidence that there was an *ex ante* reason for the monitoring. In *Nova*, a fellow employee noticed that another employee was "visibly upset" after an earlier call. In *Epps*, a fellow employee overheard the remarks that the court later determined were business-related and thus subject to recording. In *Horn*, there was no evidence of any *ex ante* justification for the monitoring of the call between the deceased and her husband; the nurse who listened-in on the call was simply being "nosey."

3. *Participant Consent Exception*

Prior to 1974, the Florida Act contained a participant consent exception similar to that in the Omnibus Act.[193] This exception provided:

> It is not unlawful under this chapter for a person not acting under color of law to intercept a wire or oral communication when such person is a party to the communication or when one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal act.[194]

This provision would have allowed parties to "intercept" their own communications without the consent of the other parties to the communication. One example would be recording business or personal conversations for later private use.[195]

A 1974 amendment replaced this provision, stating that "[i]t is lawful under this chapter for a person to intercept a wire or

---

cient occupations or avocations of their own. However, those days are gone! We now have radio and television." 298 So. 2d at 199.

192. *See supra* notes 85-95 and accompanying text (discussion of *Epps*).

193. FLA. STAT. ANN. § 934.03(2)(d) (West 1985); *Cf.* 18 U.S.C. § 2511(2)(d) (1987).

194. FLA. STAT. ANN. § 934.03(2)(d) (West 1985).

195. *See* By-Prod Corp. v. Armen-Berry Co., 668 F.2d 956 (7th Cir. 1982) (a person's desire to make an accurate recording of a conversation to which she is a party is a lawful purpose under the Omnibus Act).

oral communication when all of the parties to the communication have given prior consent to such interception."[196] Thus, the Florida Act no longer allows one-party consent: all parties to a wire or oral communication must consent for the interception to be lawful. The statute's implicit premise is that each party has an "expectation of privacy from interception by another party to the conversation."[197] The Florida legislature has shown a greater concern for protecting privacy interests in communications than Congress did in the Omnibus Act.[198]

The all-party consent provision has survived intense constitutional challenge. In *Shevin v. Sunbeam Television Corp.*,[199] media companies claimed the provision violated the first amendment by impairing news-gathering activities.[200] The media said the statute inhibited the three basic goals of investigative reporting: accuracy, candidness, and corroboration. The Florida Supreme Court held that the first amendment did not invalidate Florida's statutorily recognized privacy right.[201] The court concluded by saying, "The First Amendment is not a license to trespass or to intrude by electronic means into the sanctity of another's home or office."[202]

No court has directly addressed the issue whether the all-party consent requirement applies in situations where the requirements of the ordinary course of business exception are met.[203] The strongest argument, based on strict statutory construction, is that the "ordinary course of business" exception is just what it says it is: an *exception* independent of all other exceptions including the all-party consent requirement. It makes little sense to consider either of these two exceptions true exceptions if both must concurrently be fulfilled.

---

196. FLA. STAT. ANN. § 934.03(2)(d) (West 1985)

197. Shevin v. Sunbeam Television Corp., 351 So. 2d 723, 726-27 (Fla. 1977).

198. State v. Tsavaris, 394 So. 2d 418, 422 (Fla. 1981).

199. 351 So. 2d 723 (Fla. 1977).

200. *Cf.* State v. News-Press Publishing Co., 338 So. 2d 1313 (Fla. Dist. Ct. App. 1976) (discussed *infra* notes 206-15 and accompanying text).

201. 351 So. 2d at 726-27.

202. *Id.* at 727.

203. Diagram 2 in the Appendix demonstrates the problem. The path marked with a "?" depicts the situation where the ordinary course of business exception is met (i.e. no interception), yet participant consent would be required. This same issue has not arisen under the federal Omnibus Act primarily because *Harpel* and other cases have implicitly incorporated a one-party consent requirement into the ordinary course of business exception. *See supra* note 61. In a similar manner, Florida courts could incorporate Florida's all-party consent requirement into the Florida Act's ordinary course of business exception.

A few contrary arguments exist. The first focuses on the semantic differences between "interception" and "reception." One party to a two-party conversation does not "intercept" that communication, he simply receives it.[204] However, the 1974 amendment requires the receiver to get the consent of the other party before "intercepting" the communication. Thus "interception" as defined in the participant consent part of the statute really means "reception." Consequently, even in situations where there is only a "reception," the participant consent exception must be met. Thus, all-party consent becomes a *requisite and cumulative* provision under the Florida Act because every communication is, at a minimum, a "reception." A court addressing this issue might simply rewrite the statute by inserting "reception" into the participant consent exception where the term "interception" now appears.[205]

A second argument is that the legislative intent to protect individuals' privacy rights in their communications would be thwarted by allowing an exception for business communications. Why should business communications be exempt when other communications currently fall within the exception's protected ambit?

This issue was implicitly raised in *State v. News-Press Publishing Company*,[206] which involved the anomalous situation of a newspaper urging that its reporter's surreptitious recordings were illegal because the newspaper was indicted for destruction of evidence.[207] The evidence in question involved two tape recordings the reporter had erased following two non-consensual recordings. One recording occurred when the reporter left her recorder running without informing the two persons whose conversation was recorded. The other was a phone conversation between the reporter and another person recorded without that person's consent. The state, the newspaper and the court agreed that recording the first conversation was illegal.[208]

204. Chiarenza v. State, 406 So. 2d 66, 67 (Fla. Dist. Ct. App. 1981). *See also* Inciarrano v. State, 447 So. 2d 386, 388 (Fla. Dist. Ct. App. 1984), *rev'd in part*, 473 So. 2d 1272 (Fla. 1985).

205. The term "reception" does not appear in the statute. Also, the legislature's failure to use the more expansive term "reception" in modifying the participant consent exception could be intended to preserve the viability of the Florida Act's other exceptions.

206. 338 So. 2d 1313 (Fla. Dist. Ct. App. 1976).

207. *Id.* at 1314-15.

208. *Id.* at 1315.

However, the state argued that the second recording was not illegal because no interception occurred.[209] The court rejected this argument, holding that the recording was illegal.[210]

Apparently, neither party argued the ordinary course of business exception.[211] So the court addressed only the participant consent exception.[212] In addition, the court's analysis was flawed because it relied on the definition of an "oral communication" in analyzing whether the recording of a telephone conversation — a "wire communication" — was illegal.[213] Finally, the context of *News-Press* is different from the ordinary telemarketing situation.[214] Nevertheless, the court's tenor was clear: the legislature intended each party to a communication to have an expectation of privacy from interceptions by other parties.[215] This theme is repeated in other Florida cases,[216] so it seems likely that arguments for applying participant consent requirements to business communications will prevail in Florida.

C. Phone Company Tariffs

State regulation of telecommunications gives further protection to privacy interests. In Florida, telecommunications companies regulated by the Florida Public Service Commission are required to include in their service tariffs restrictions against certain practices. In Southern Bell's current service tariff, customers are permitted to use voice recording equipment only when specific criteria are met.[217] First, the user of the recording equipment must be able to activate or deactivate the equipment at will. Second, the customer must acquire some form of consent from all parties to the recorded conversation. The cus-

209. *Id.*

210. *Id.* at 1316.

211. The newspaper was not an effective advocate for the business community because it wanted to disassociate itself from the employee's activities by arguing that they were illegal.

212. Shevin v. Sunbeam Television Corp., 351 So.2d 723 (Fla. 1977) would probably override an argument based on the ordinary course of business exception. This assessment follows because in *Sunbeam Television* the Florida Supreme Court rejected the media's arguments, which relied on federal constitutional authority (i.e., the first amendment), not a statutory exception.

213. 338 So. 2d at 1316.

214. *Id.* (court took notice of the case's unusual circumstances).

215. *Id.* at 1316.

216. *See, e.g.*, Shevin v. Sunbeam Television Corp., 351 So. 2d 723 (Fla. 1977).

217. General Subscriber Service Tariff, Southern Bell Telephone & Telegraph Company, A.15.1.1(D) (June 16, 1986).

tomer may do this in three ways: (1) prior consent may be obtained in writing; (2) prior consent may be part of, and obtained at the start of, the recording; or (3) a distinctive recorder tone repeated at intervals of about fifteen seconds may be used to alert parties when recording equipment is in use. The tariff also contains some exceptions generally unrelated to business monitoring.[218]

Under the tariff agreement, individual phone companies are responsible for enforcing the tariff provisions against their customers. If Southern Bell learns that one of its customers is using recording equipment in violation of the tariff agreement, Southern Bell must take immediate action by promptly asking the customer to discontinue the use of the equipment or correct the violation. Within ten days of notification, the customer must confirm in writing that he has complied with the company's request. Telecommunications service is suspended until the customer complies with the tariff's provisions.[219]

A telephone company that fails to enforce its tariffs could be subject to fines or the amendment, suspension, or revocation of its service certificates. The Commission has the power to order the company to enforce the tariff's provisions. The Commission may also impose a penalty of up to $5000 for violation of the Commission's orders.[220]

In summary, phone tariffs impose an additional hurdle on the recording of telephone communications. Current tariff provisions in Florida parallel those the FCC imposes, requiring some form of all-party consent. The tariffs, through economic pressures, compel the telephone companies to safeguard the privacy interests of their customers from non-consensual recordings.

Conclusion

Both the monitoring and recording of telephone communications are permissible if done within certain guidelines. FCC regulations, phone company tariffs, and state rules such as Florida's all-party consent requirement all hinder the recording of phone communications. Failure to adequately fulfill the

218. *Id.* at A.15.1.1 (D)(3).

219. *Id.* at A.15.1.1 (E).

220. FLA. STAT. ANN. § 364.285 (West 1985) (telephone companies); *Id.* § 350.127 (regulated companies generally).

dictates of federal or state law not only subjects a violator to civil and possibly criminal sanctions, but also does damage to its public and personnel relations. Thus, businesses should develop plans that strictly adhere to federal and state guidelines.

A. Monitoring

A business is permitted to monitor phone communications transmitted from or received on its phone system under the ordinary course of business exceptions contained in both federal and Florida law. However, there must be a legitimate business need for the monitoring. Examples of legitimate business purposes are (1) prohibiting the unauthorized use of telephones, (2) protecting the company from disclosure of confidential information, (3) dealing with irate and abusive customers, and (4) supervising and training new employees in dealing with the public.

Two other rules, however, also apply. First, employees should be directly notified. Surreptitious monitoring is not permitted under any circumstances. Constructive notice is likely to be ineffective because it does not reduce employees' subjective expectations of privacy. Instead, the employer should give written notice, preferably signed by the employee. Under federal law, one-party (i.e., employee) consent is sufficient for monitoring to occur. Under Florida law, however, resolution of the issue is more difficult because of the state's all-party consent requirement. The *Nova*[221] and *Tsavaris*[222] cases suggest that only one-party consent is required under the ordinary course of business exception. However, the *Sunbeam Television*[223] and *News Press*[224] cases provide strong arguments to the contrary. A Florida court confronted with this precise issue will have to consider whether following the Florida trend towards expanding privacy protections effectively destroys the ordinary course of business exception. Perhaps the Florida courts would carve out exceptions similar to those federal courts have recognized.

Second, monitoring personal calls is generally prohibited. This area is the most perilous. The fundamental rule is that a

221. 361 So. 2d 411 (Fla. 1978).

222. 382 So. 2d 56 (Fla. Dist. Ct. App. 1980), *review denied*, 424 So. 2d 763 (Fla. 1983).

223. 351 So. 2d 723 (Fla. 1977).

224. 338 So. 2d 1313 (Fla. Dist. Ct. App. 1976).

business may monitor calls that are "reasonably related to a business purpose." A call's content is important. If the content is business-related, most courts allow the call to be monitored. Personal calls may be intercepted to guard against unauthorized use of the telephone or to determine whether a call is personal or not. If a call is determined to be personal, the interception must be terminated within a brief time (about fifteen seconds).

However, a prudent policy to monitor only those communications that are clearly within the core of business-related communications. For example, one case[225] held that an employer had no legal interest in an employee's conversation with a friend over the employee's prospects of employement elsewhere. An employer may feel such information is business-related, but it is also protected under the employee's privacy rights. Examples of core business communications would include disclosures of company secrets and communications directly related to a company's business transactions and dealings with the public.

B. Recording

Recording is permitted under basically the same guidelines that apply to monitoring, with one large difference. FCC rules, phone company tariffs, and state laws like Florida's all-party consent requirement do not provide for one-party consent to recording. Under FCC rules, telephone communications may be recorded if there is (1) a beep tone, (2) consent of all parties, or (3) notification. None of these options would be favorably received by consumers calling a business seeking information or assistance. Phone company tariffs and Florida's all-party consent requirement also inhibit candor, spontaneity, and openness of communication.

It is uncertain whether an employer can record communications under the ordinary course of business exception without all-party consent. One argument is that once the ordinary course of business exception applies, the all-party consent requirement does not apply. Even if this argument prevails, the FCC and phone company tariffs are remaining hurdles.

Under the Florida Act, the subscriber does not have the option of obtaining recording equipment from sources other than

225. Watkins v. L. M. Berry Co., 704 F.2d 577 (11th Cir. 1983).

the phone company. However, under one federal case, *Epps*,[226] recording equipment was held not to be an "intercepting" device.[227] Under the rationale of *Epps*, only the intercepting device (the telephone) must be acquired from the communications provider. A prudent strategy for Florida businesses would be to purchase or lease recording equipment from the telecommunications service provider.[228]

C. Instituting Safeguards to Protect the Employer

A cautious employer should implement certain safeguards before monitoring or recording calls. The following are four suggestions.

First, directly inform all employees that call monitoring or recording will be occurring. This notice forewarns employees of the surveillance and minimizes any expectation of privacy they may have on company phones. The notice should thoroughly describe (i) the time periods during which monitoring or recording can occur; (ii) the particular phones the company plans to monitor or record; and (iii) whether incoming or outgoing calls will be monitored or recorded.

Second, institute procedures outlining (i) the persons who may conduct monitoring and recording activities; (ii) the methods by which monitoring or recording may be done; and (iii) the circumstances in which monitoring or recording may be done. Procedures for monitoring or recording personal calls should be particularly definitive. The employees conducting monitoring or recording activities must be directed to terminate interception of a personal call, regardless of the call's contents, within the briefest period of time necessary to identify the call as personal. Once a call is determined to be personal, the interceptor must hang up.[229] However, if employees are informed that the entire content of all conversations is recorded, the employees' consent requirement is probably met.

Third, company policy should specify the purposes for the monitoring or recording to prevent any inference that the company is engaging in "eavesdropping" without identifiable rea-

226. 802 F.2d 412 (11th Cir. 1986) (discussed *supra* notes 85-95).

227. *Id.* at 415.

228. However, some other states have provisions similar to the Omnibus Act which allow users to purchase their own equipment. *See supra* note 158.

229. This requirement may be impossible to fulfil if all calls are mechanically recorded.

sons. The policy should also establish guidelines for documenting an employee's unauthorized use of company phones. Employers seeking to discipline or terminate employees for violations of company policy must possess substantial documentation to support sanctions or discharge, particularly when a wiretapping claim is likely to result. Additionally, the use or disclosure of the contents of monitored or recorded communications could result in tort liability for invasion of privacy where the use or disclosure is unlawful or unrelated to a legitimate business purpose.

Finally, whenever possible, employees should be provided with a phone for personal calls that is insulated from the monitoring and recording systems.[230] This segregation of phones minimizes the issue of whether a call is "business" or "personal"; at least there is greater justification for an employer monitoring or recording any call on the "business" phones in such a situation because employees would have little reason to use the business phone for personal purposes.

230. *See* Simmons v. Southwestern Bell Telephone Co., 452 F. Supp. 392, 395-96 (W.D. Okla. 1978), *aff'd*, 611 F.2d 342 (10th Cir. 1979) (court found it significant that unmonitored phones were available).

Appendix

Diagram 1
Liability Under the Omnibus Act

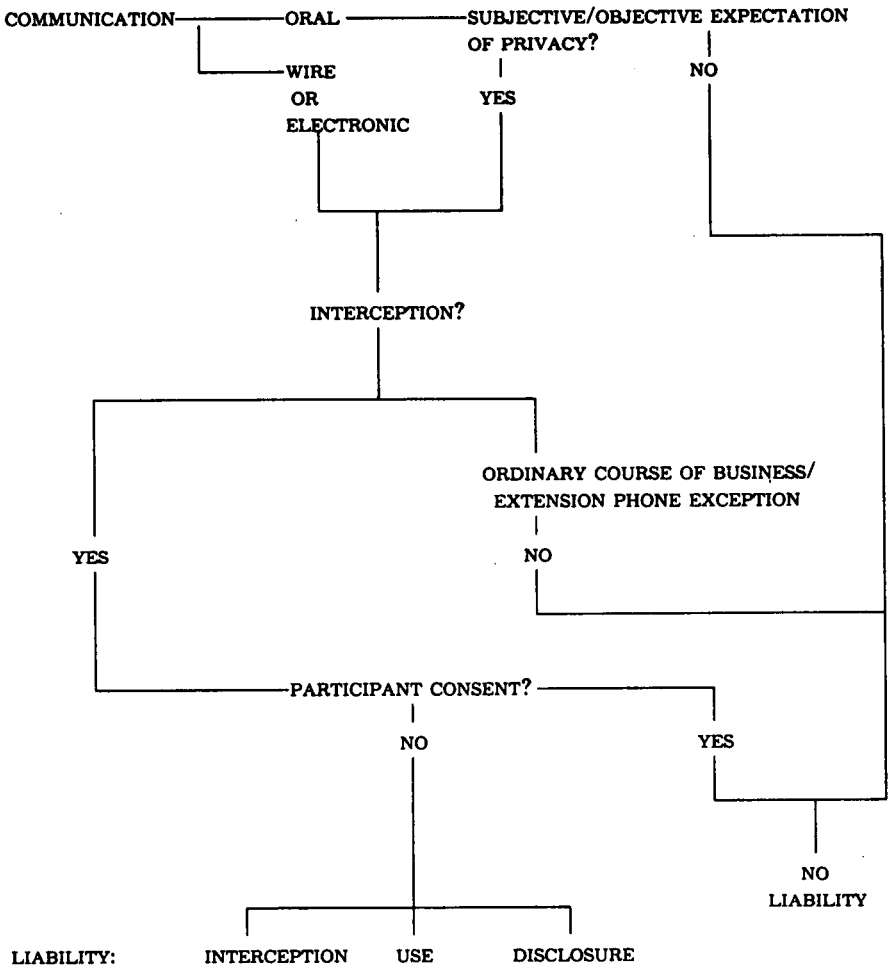

Diagram 2

Liability Under the Security of Communications Act